REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	7.Jan.99	MAJOR REPORT

4. TITLE AND SUBTITLE
BUSINESS CONTINUITY PLANNING

5. FUNDING NUMBERS

6. AUTHOR(S)
CAPT CORBITT SCOTT M

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
GEORGE WASHINGTON UNIVERSITY

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
THE DEPARTMENT OF THE AIR FORCE
AFIT/CIA, BLDG 125
2950 P STREET
WPAFB OH 45433

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
FY99-10

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited distribution
In Accordance With AFI 35-205/AFIT Sup 1

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS

15. NUMBER OF PAGES
36

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

Corbitt

ABSTRACT

All organizations are dependent on People, Information, and Communications to conduct business. Interruptions that affect any of these resources will have a detrimental impact on business. Disasters that affect these resources will likely have a far-reaching impact on business and may result in the failure of the business or organization. Business must plan for continuing business after a disaster via a Business Continuity Plan. The BCP is a critical function of the business and will impact every function of the business. Planners must have resources and commitment from senior executives to be successful. Planners must develop plans that recover time sensitive functions first, while bringing less time sensitive functions on line in an economically balanced manner. Planners must consider the toll of a disaster, not only on their facilities and equipment, but on the human resources which are their most precious asset. Planners must ensure plans are maintained and exercised on a regular basis and critique the exercise participants to improve their chances for successful resumption of business. Organizations that are led by strong leaders with genuine concern for their customers and employees will develop strong continuity plans. Overall the private sector is more advanced than government when it comes to BCP, however some large corporations still lack integrated continuity plans.

BUSINESS CONTINUITY PLANNING

Scott M. Corbitt
21 Aug 1998
Forensic Science 295
George Washington University
Professor Lloyd F. Reese

DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

Organizations have become dependent on their information systems and their ability to process data to meet their mission, goals or customer/client needs. Today, business is conducted with greater speed and interconnectivity than ever imagined. However, these two factors that drive and fuel business are is also threats to business survival if operations are interrupted or suspended. A University of Texas study found that 85 percent of businesses are totally or heavily dependent on information systems to stay in business.[1] Disruption of automated systems even for a few days could cause severe financial loss and threaten survival of the organization.[2] To meet this threat, organizations should develop Disaster Recovery Plans or Business Continuity/Resumption Plans. Like most areas that are continually developing, this field has moved from planning for recovering Data Centers from disasters to full Business Resumption Planning. While many organizations have built recovery programs for their data centers and key application platforms, the balances of their enterprises are increasingly at risk.[3] The risk is widespread as a study conducted by Comdisco, a corporation supplying recovery planning and programming for clients, found only 12 percent of organizations have an effective Business Continuity Plan in place.[4]

What is a Business Continuity Plan?

A Business Continuity Plan or BCP is a complex set of analyses, preparations and procedures with a single goal: Keep the business running after

a disaster occurs while helping it resume normal operations as quickly and intelligently as possible.[5] A Business Continuity Plan is not an inventory of existing systems or a guidebook for duplicating those systems. A BCP is an action plan for providing key corporate functions with the required capabilities when they are needed.[6] A BCP has three goals:

1. **Minimize Potential = Crisis Prevention**
2. **Emergency/Crisis Management**
3. **Resumption of Business Activities**

How Did Business Continuity Planning Start?

BCP began in 1973, as an attempt to document step by step actions and procedures required for recovery of a Data Center after a software or hardware failure.[7] The initial focus was on software development to solve the problem, which quickly developed into full-scale written and documented plans to recover the data center disaster.[8] In late 1979 the first ***"hot-sites"*** became available (commercially available vendor to which a company can move computer operations on a temporary basis while their primary site is being recovered).[9] The Data Center Recovery Plans took on new focus after a Norwest Bank fire in 1983, which gutted 7 floors of the bank in Minnesota.[10] In May of 1983, The Treasury Department required banks to have documented plans for resuming operations if they used a computer anywhere in the operation.[11] Auditors then began to make findings about lack of resumption planning in non-computer operations in banks and financial companies outside of banking such as

brokerage firms.[12] Similarly, CEOs began to have real concerns about revenue generating functions of their businesses and the development of Crisis Management Plans was the result.[13] Crisis Management Plans were relatively weak and were after the fact oriented. Crisis Management Plans detailed what would be done, but gave no considerations to facilities, equipment, personnel, or detailed execution.[14]

Organizations became strapped with a Crisis Management Plan, Emergency Response Plan and a Data Center Recovery Plan, all of which were owned by different offices with limited interaction.[15] The BCP developed from this dysfunctional array after CEOs were convinced that all of the functions of Security (Emergency Response), Business Resumption, and Information Systems Recovery should be place under one Business Continuity Program, with one leader and manager. [16]

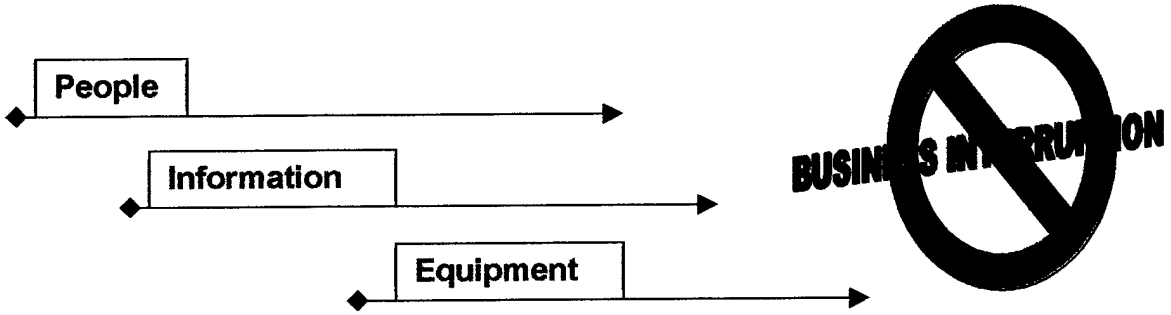
Why is a Business Continuity Plan Needed?

The need for a BCP should be obvious to every person in an organization, however this is often not the case. Some organizations have extremely capable plans in place and exercise the plans accordingly. Other organizations have failed to plan, or have reduced the budget of the BCP function in cost cutting measures. BCP is not an operational aspect of an entity until an actual disaster happens, hence with disasters being few and far between, little attention is paid to the BCP function.[17] Business Continuity Planning is also expensive, and

management is always more interested in funding current business operations. Organizations that have effectively planned for a disaster have realized the importance of Data Centers and like functions to their operations. Large companies that are moving towards total Business Resumption Plans have realized that their information systems represent everything they do in their business.[18] Information systems are central to operations and play a large role in protecting an entity's assets; service continuity is really a part of the larger security umbrella.[19]

An important part of establishing the need for a BCP is to assess the criticality of systems to operations. The BCP protects the three axes of recovery planning; people, information and equipment. Knowing how these three elements work together to meet company goals and to perform daily operations is critical to successful Business Continuity Planning.[20]

21



What are the Risks?

Risks to interruption of routine business functions abound, not only for businesses and corporations but also for all levels of government. Some examples of the risk to government were highlighted in a November 1997 GAO

Report on Information Security Management. The risks included law enforcement reliance on the FBI maintained National Crime Information Center computerized database, the Customs Service dependence on automated systems to process and inspect billions dollars of imports on a daily basis, and the reliance of the Social Security Administration on systems to disburse government entitlements. Compounding the problems is the fact that each governmental unit has systems that are interconnected to form networks or are accessible through public telecommunications systems.[22] The damage of an outage quickly becomes overwhelming.

On the commercial side of the ball, a one week interruption in operations for many industries will not only interrupt cash flow, but may ameliorate a client base and could cause regulatory and legal failures as well. The University of Texas study claims that only 6 percent of companies suffering from a catastrophic data loss survive, while 43 percent never reopen, 51 percent close within two years of the data loss.[23] A similar study conducted by the University of Wisconsin determined that 43 percent of businesses never reopen after a local disaster and 29 percent close within two years of a local disaster.[24] Business Continuity Plans therefore become necessary for every business from a family owned restaurant to a Wall Street brokerage house.

What Drives Businesses to Plan for Business Continuance?

Over the last 2-3 years corporations have begun full scale Business Continuity Planning, expanding their emergency response and life safety plans to address resumption and continuity of time sensitive and less time sensitive business and service operations.[25] Although there is some disagreement between experts about the cause for this robust interest in BCP however, it is significant to note that the organizations did not begin planning until the impact of a business interruption could be demonstrated to them. The corporations were not moved by auditor findings or best practices recommendations.[26] Legal and Regulatory requirements generally resulted in de minimis planning to satisfy the requirements, however companies that have experienced a disaster have **"real"** plans.[27] The demonstration of potential business loss due to interruption caused by a disaster was the key factor in moving organizations towards BCP.

Senior Executive Involvement versus Commitment

A key development in the move towards BCP is the movement of management responsibility up the chain towards senior executives.[28] This is not only the result of mandates by the government, but because of "duty of trust" and "due diligence" required of officers and directors by stockholders.[29] This fact will prove critical in obtaining senior executive support for Business Continuance Planning, exercising and funding. Corporations with the best plans have CEOs that have a high awareness of the business needs of customers and are aware

of the personal needs of their employees.[30] Companies that are led by forward thinking leaders that never want their customers to criticize their operations or have negative publicity due to the impact of a disaster, will generally have strong Business Continuity Planning.[31] Executives must be committed to BCP rather than merely involved.

The Cost of Downtime

Average Financial Impact of One Hour of Interrupted Computer Operations	
Retail Brokerage	$6.45 Million
Credit Card Sales Authorization	$2.6 Million
Catalog Sales Centers	$90,000
Airline Reservations	$85,500
ATM Service	$14,500

[32]

CHALLENGES TO PLANNERS

Senior Executive Support

Business Continuity Planners must have active Senior Executive support for their efforts. Senior Executives will champion the effort and carry the banner for the planners.[33] Only with Senior Executive support can planners expect and receive the required participation of the various business units needed to make the plan functional. Planners likewise must be able to demonstrate to the executives how they will benefit from the planning and in the end how they will win.[34] "Most senior managers are optimists by nature. They look beyond obstacles and focus on opportunities. There is little appeal for them in looking at infinitesimally small likelihood of huge disasters. On the other hand, keeping management focused on an effort that will address the safety of the

organization's people, mitigate the impact on customer services, and maintain the financial well-being of the company are much more powerful motivators for senior management."[35]

Integration of Multiple Business Units

A BCP is only effective if its control spans the breadth and width of the corporation it serves. Obtaining cooperation from many different functional areas within a corporation, especially a large diversified Fortune 500® corporation that is globally operational, is a tremendous challenge. Many corporations have just begun the shift to BCP or resumption planning and will be faced with unprecedented integration problems. A true BCP will replace existing non-integrated Emergency Response Plans, Data Center Recovery Plans and Natural Disaster Plans. These existing plans may or may not be in a written format, and business units may be unwilling to allocate the time necessary away from day to day operations to help write plans for their unit. The response from many business units will be similar to 'Why should we plan and write it down? We know what to do if X and X happens!' Although planners should expect initial resistance they must persevere to accomplish the plan and exercise it accordingly.

Keeping Plans Current

Organizations are changing almost daily in our world. Computers and technology change rapidly, and personnel will change positions on a regular if

not frequent basis. Everything in a plan needs to be systematically reviewed by the business unit and submitted to the planners for appropriate changes. The plan should be a "living" document. Changes that are not reported will likely cause a delay when a disaster strikes. Imagine a plan that is just over a year old, but is worthless, as numerous personnel have changed as well as the organization's cellular telephone provider. At a minimum the plan should be thoroughly scrubbed and exercised semi-annually.

Finding the Budget and Keeping It

Although Business Continuity Planners are a fairly talented bunch, they will still need a budget large enough to support their efforts. Developing and implementing a plan will cost money, as will updates to the plan, exercises, and the hiring of outside consultants to assist at various stages of plan development and maintenance. Other vendors to the plan such as hot site providers do not work for free, and the plan should also include the method of obtaining immediate funds to initiate resumption efforts at the zero hour.

In comparison to the global budget for a corporation, the BCP budget is generally a small percentage[36]. However, it must come from somewhere, and in the initial phases of the planning effort, it will likely be reallocated from within the existing budget, or from specially allocated funds procured by the senior executive responsible for plan development. After budgets are developed and allocated on a fiscal year basis, planners should prepare for a constant assault

on its justification. As businesses continue with cyclical downsizing, budget cutting and attempts to improve the bottom line (especially in light of recent earnings decreases), continuity planners will be competing for budget with other business functions.

Plan Construction and Development

THE BUSINESS IMPACT ANALYSIS

Every organization should start their BCP process by conducting a complete and comprehensive Business Impact Analysis (BIA). A BIA involves identifying the critical business functions within an organization and determining the impact of not performing the functions beyond the maximum acceptable outage.[37] The BIA will become a very important document because it will quantify the loss of revenue, loss of shareholder confidence and negative public image developed as a result of a disaster or outage. The BIA is the document that will be presented to management and will be the document that will be the cornerstone of the Business Continuity Plan.

The planners must include in their Business Impact Analysis the risk that a full range of disasters poses to the organization. The disasters are not limited to natural or human threats, but must also include technical risks to computing and other facilities. Planners will also be concerned with events that may pose no threat to the physical structure or integrity of the facilities but may prohibit the workforce from coming to work (blizzard, damaged bridge, etc). All units that are needed for a time sensitive function must be identified in addition to the unit that

has primary responsibility for the function. Thus, one unit may be primarily responsible for a Time Sensitive Function (TSF), but if it is dependent on other units to accomplish the TSF, the other units must be identified and incorporated in the BCP. Interdependency between business units must not be overlooked.

Types of Threats	Types of Events
Natural Threats	Flooding, Fire, Seismic Activity, Winds, Snow and Ice, Volcanic Eruption, Tornado and Hurricane
Technical Threats	Power Failure/Fluctuation, HVAC Failure, Failure of CPU, Software Failure, Telecommunications Failure, Gas Leaks, and Electromagnetic Pulse (nuclear or otherwise)
Human Threats	Robbery, Bombing, Embezzlement, Extortion, Executive Kidnapping, Burglary, Vandalism, Terrorism, Civil Insurrection, Chemical Spill, Sabotage, War, NBC Contamination, Vehicle or Airplane Crash, and Labor Strike

The critical needs of each department within the organization must be carefully evaluated. Functional Operations, Key Personnel, Processing Systems, Service Provided, and Critical Record Keeping should be included in the evaluation.[38] An organization must make a robust effort at analyzing their daily functions. A thorough BIA will provide a detailed record of daily activities to the planners, activities that may be transparent to the corporate executives and the employees who execute them, but are actually critical to the success of the organization on a daily basis. An analysis over a two to four week period can indicate the principle functions performed inside and outside the department.[39]

To determine critical needs numerous questions must be addressed during the Business Impact Analysis. Questions such as "If a disaster occurred, how long could the department function without the existing equipment?"[40] Other

questions will identify the high priority tasks; to include manual functions and processes in the area and the frequency of the tasks performed. The analysis will also address equipment and staffing needs to perform the essential functions, and the process for replacing them in a disaster. Planners must also address any "outsourced" functions that are performed by vendors or contractors. Even off-site vendors may lose their ability to perform in the event of regional disasters.

Prioritization of Functions

Prioritization of the critical functions is also important. The planners will follow the prioritization list while building the BCP plan. Since the BCP is an action plan, the prioritization will be the first document that describes what the order in which functions will be rejuvenated after the disaster. Critical functions can be further divided into three categories.

Critical Function Categories	Description
Essential	One Day Disruption=Serious Jeopardy
Recommended	One Week Disruption=Serious Jeopardy
Non-Essential	No Serious Detraction from Operations

[41]

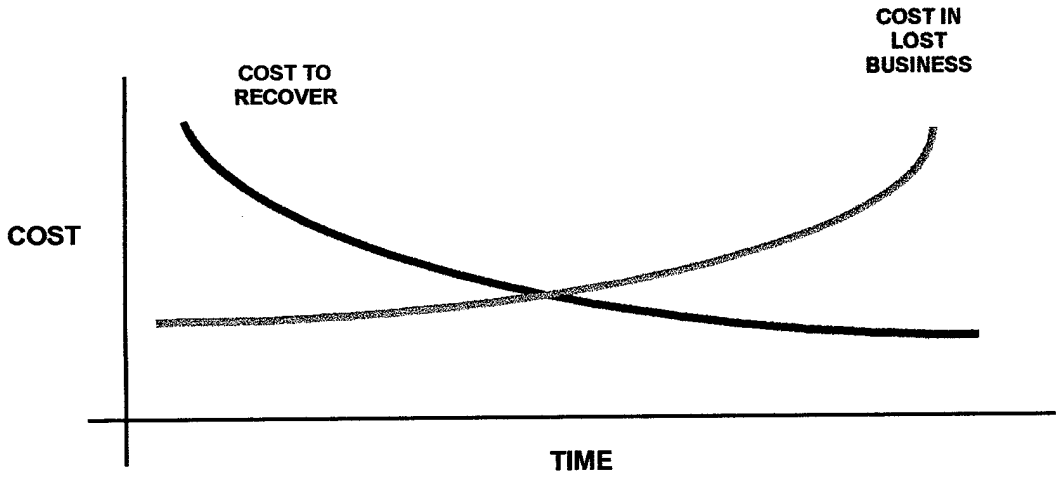
Another way of prioritizing functions for scheduled recovery and resumption after a disaster is indexing. This uses a similar program, however it enables planners to move away from a type of language that has become unfashionable. Critical functions may be non-essential after a disaster. Preparing a balance sheet is a critical function at the end of an accounting cycle, but it can, if necessary, be delayed for several months.[42] By placing it in the

above categorization it would be considered non-essential, which misplaces the importance of the function. Indexing will break down operations of the entity in the following manner.

Rating	Description	Examples
Vital (high)	Operations that support company cash flow Operations that provide customer service and support	Accounts Receivable Payroll Ordering Billing
Important (medium)	Operations that support ongoing Company business functions Operations that maintain records for legal, accounting and tax purposes	Accounting Auditing Production Scheduling
Deferrable (low)	Operations that provide internal company services Operations that are developmental in nature	Sales Reporting Instructional Systems Modeling

[43]

After the occurrence of a disaster there are two assets available to recovery personnel; time and money.[44] Recovery personnel must spend both wisely, if personnel spend time and money doing the wrong thing, both assets will be lost.[45] After a disaster is when the time spent doing a Business Impact Analysis will pay off. The BIA will provide an economic impact model that will help determine how fast resources are recovered based on expected business loss.



Although the cost and timelines will vary for each and every business, and potentially each function in the business, the model will help executives make decisions prior to the disaster about what functions will be regenerated based on a cost-benefit analysis. The BIA findings will determine what are the recoverable units or functions and how long the company can wait to bring units or functions back to operational standards.[46]

BCP: The Plan

The BCP is the most important function for organizational survival after a disaster. A proper plan will provide the guidance, direction, and actions required to survive a crisis and resume operations. Plans must be developed for individual, regional and national level disasters. Planners must consider that the primary facility may be non-functional or that access may be restricted due to safety concerns or to support forensic and law enforcement investigation. Planners should at a minimum plan on being kept out of their facility for several days. However, the delay for entry may actually be several weeks, such as was the case for businesses located near the Murrah Federal Building in Oklahoma City.

The first component of the plan is the development of an Emergency Operations Command and Control function. This is generally manifested in an Emergency Operations Center. The EOC Chief is a senior executive, and is supported by personnel from every business function. The EOC Chief must be

empowered with the requisite authority to recover the organization. This authority will include not only the ability to draw upon internal corporate resources at a moment's notice, but also the authority to bind the corporation contractually for required services from vendors and suppliers. The EOC must also include a representative from the General Counsel, and an accountant to track funds spent on recovery efforts.

Subordinates to the EOC are Situation Assessment Teams (SATs). These teams are responsible for determining the level of loss for the organization and reporting accurate information to the EOC, so options may be executed. SATs will be comprised of information technology personnel, personnel from different business units, and facilities engineering personnel. SATs will not only perform visual inspections of work area, but will also run technical tests and examination of Data Centers and Network Information Systems if appropriate. SATs are the eyes and ears of the EOC Chief.

Data Center Options

Plans must be developed for resuming operations if the data center has time sensitive functions. Several options exist to help a data center recover from a disaster or outage. Movement to a hot site is a preferred option. Some corporations have developed and built their own internal hot site, which is a duplicate facility, ready for operation with minimum notice. These sites are initiated with the most current data stream available from back-up data.

Maintaining an internal hot site is very expensive and the majority of companies will seek other options for data center recovery.

A vendor provided hot site enables an organization to move their data center in a few short hours. Hot site vendors may also provide interim work areas equipped with computing and related materials for non-data center employees. Vendor provided hot sites are functional, but on an anecdotal aspect, vendors have never been strained by a regional or national disaster. Hot site vendors can support a plan, however they may not be able to provide an organization with their preferred location during regional or national disasters. Hot site vendors generally charge a contract origination fee, per day usage fee and a disaster declaration fee. The disaster declaration fee for a large organization is generally quite sizeable ($25,000 to $30,000) to prevent organizations from premature declaration. The fee is designed to prevent organizations from arbitrarily and unnecessarily declaring a disaster. This fee causes organizations to perform an economic cost/benefit analysis prior to declaring a disaster. The fees in totality initially seem quite expensive, but are minimal when compared to a large business outage or the cost of maintaining an internal hot site. Lastly, planners must ensure that any vendor associated with resumption efforts must also have a BCP and specifically address how they plan to support their clients in case of a disaster.

Other options exist for data center recovery. Corporations may build ***"Warm Sites"*** at other geographic or regional locations. Warm sites are facilities designed for use as a replacement for data centers or other operations, but are able to be used for less critical functions during the normal course of business. Functions such as training, research and development, and product testing are good daily uses for warm sites. These functions are important, but a delay caused by a disaster elsewhere and arrival of time sensitive functions will not cause the organization significant stress in most cases. Another option is the sharing of disasters between corporations or organizations. In this scenario, corporations with similar computing facilities would agree to support each other in a disaster. A corporation that is in the midst of a disaster could reach out and gain access to another entities facilities to run their data and support their time sensitive business. This option reduces a corporation's autonomy, and makes the company dependent on another business for supporting the corporation. The upside to these agreements is that they are inexpensive to maintain; however planners should not be entirely dependent on the promised support.

"Cold Sites" are the last option available to planners for Data Center recovery. A cold site is simply a facility that is maintained with adequate power, HVAC and telephone and data lines to support rapid development of a data center. Computers for a cold site will not be in place, but must be provided during resumption activity. Planners can develop contracts with vendors to provide emergency computing equipment in a very short period of time. The

computing equipment can arrive pre-loaded with software in as little as 24 hours. Planners can expect to pay hefty premiums for such service if it is ever required.

Work Area Options

Many disasters can not only damage your data center, but also leave your workforce without a center if facilities are damaged, contaminated or otherwise inaccessible. Work Area options are similar to the data center options. Planners can find space in the local rental market at the time of disaster or can shift to other facilities in the local region or outside the region if transportation is available. Corporations that have larger manufacturing or warehousing facilities can implement plans to convert unused space on a temporary basis. A temporary conversion of warehouse facilities to a work center is one option, with installation of sufficient HVAC, rented office furniture, and telecommunications. The Warehouse function could then be moved to office trailers and storage trailers on a temporary basis. If a facility is only partially inaccessible, but otherwise meets life code requirements, a company could simply furlough less time-sensitive function employees and allow the more time-sensitive functions to operate out of the available space. Budget and logistics are the primary factors when assessing options for temporary workspace.

Dual Centers

Many companies find that being out for just a few minutes to be unacceptable. Brokerage Firms, Mutual Fund Companies and Banks are a few

of the industries who would suffer severe revenue loss if customer service capabilities failed for even a few hours. Catalog Retailers and Direct Merchants are other good examples of companies that would suffer significant revenue loss if customer orders are not able to be processed in a timely manner. Certain of these companies have diversified their risk by opening duplicate customer service centers in geographically separated areas. One particular unnamed organization has facilities in the Northeast and in the Southwest of the United States. If an outage occurs at one center, workload is shifted to the other operational center.

Work Force Concerns and Contingencies

It is critically important for planners to understand that workers may not be immediately available after a disaster to resume business operations. Disasters in which lives were lost such as bombings or natural disasters that have resulted in the destruction of employees homes and the displacement of their families will likely cause significant disruption to resumption attempts. Companies should be prepared not only to help themselves, but also to help their employees resume their normal lives as quickly as possible. The faster the employees are able to resume a standard of normalcy; the better of the company will be as the employee will be available to do his or her job.

Companies can provide temporary cash disbursements to meet workers day to day living needs, as many locations will lose ATM service and Banks may

not be functioning properly. Companies can also provide help with filling out insurance claims for employees' personal losses and provide loans to assist with longer-term needs. One company, whose facility was left unmarred by a hurricane, allowed disaster stricken employees to bring their families in to use lavatory facilities. Employees returning to work were also allowed to bring children and pets with them until their lives resumed normalcy. These two factors were critical in resumption of normal operations, the employees realized that the company did care about them personally, and as a result felt a duty to help the company resume operations.

Dispersal of Business Functions

In circumstances where it is apparent their will be significant lag time to resumption, a facility can disperse its functions to company assets in other areas. Hence if a facility in Washington DC were destroyed by flood, the function could be transferred to a facility in Ohio until resumption is achieved. It is likely that the gaining facility would be unable to completely support the new workload in its entirety, thus employees from the disrupted facility would likely need to travel to the gaining location. Businesses relying on such a plan, should pre-identify personnel who would be available for extended travel and the company should be prepared to pay dislocation allowances and bonuses as appropriate. One business that utilizes this type of planning has exercised the concept by switching business functions between Washington DC and Philadelphia PA for a two week period. Although this caliber of exercise is very expensive, it provided

Business Continuity Planners with the opportunity to demonstrate their function to the company on a grand scale.

The Written Plan

The written Business Continuity Plan will be a voluminous document that will embrace every component of a company. Although each component or business unit's actions before, during and after a catastrophe will be delineated in the text, it is important to realize the end users will probably never read or use the comprehensive plan. End users will be provided shorter, unit specific action guides, these guides will be written in a concise and executable format to ensure easy understanding and immediate execution. The plan and all action documents must be updated on a regular basis.

Tips for Plan Development

- **Write Plans designed to recover from all possible disasters impacting a company or organization**
- **Insist that all vendors and BCP service providers all have BCP or similar plans**
- **Construct and Distribute Notification Lists and Telephone Trees for each business unit**
- **Consider having EOC duty lists for weekends and holidays**
- **Determine Disaster Declaration Parameters and Identify persons with authority to Declare Disaster**
- **Establish a Timeline for Determining Hot Site Activation**
- **Ensure back-up facilities are available and appropriately modified**
- **Identify and Pre-Position Critical Resources**
- **Include Legal, Public Affairs, and Accounting as part of plan**

Internet Web Site Contingency Planning

A new and growing area of concern in the information technology world is web site contingency planning. Companies are expanding their web sites from simple advertising of product, to interactive ordering and sales functions. A Company pursuing and utilizing electronic commerce via a web site could lose tremendous revenue if their web site malfunctions. In the future, contingency planners must consider web-based activities in their planning.

Business Continuity Exercises

The final plan should provide for semi-annual Business Continuity Exercises. Planners should prepare a tabletop demonstration of exercise plans to senior management prior to initiation. The demonstration will allow management to envision what business areas will be exercised and will enable the scheduled EOC Chief to begin to understand his role in leading the exercise more clearly. Each exercise should use a different disaster scenario and must be conducted under as realistic circumstances as possible. The old colloquial of "sweat more in training, bleed less in war" can be amended to "spend more on the exercise, and lose less revenue during disasters".

Back Ups and Vital Records Recovery

The text of this paper has previously stated that a company is dependent on its data, and that data is an asset, which needs to be protected. Electronic media should be backed up at regular intervals and stored off site. The interval

at which data is backed up depends on the size and type of business. Small businesses may only need to back up data once per week, while large banks may continually back up data and store as many as 500 tapes off-site everyday. Off site storage is also important as it prevents your back up data from being compromised at the same time as the rest of your information and systems. What good are back up tapes if they are stored next to the mainframe that was just flooded by a freak natural event? Small business owners may find a simple bank safe deposit box to be effective. Larger business may use a vendor that is in business for the express purpose of storing and safeguarding back-up data. These vendors provide pick-up and retrieval services and provides emergency delivery in event of a disaster.

Electronic Vaulting

Electronic Vaulting is fast becoming another popular way of storing large amounts of data off site. It is a process by which data is transmitted from a facility to a back up site electronically. There are several advantages in that there is no longer a transportation threat to data, and the data is sent off site immediately lessening the time back-up data awaits transport. Electronic Vaulting services can then store your data on tape and remove it for off-line storage. A Company needs to ensure that their service does in fact remove the data from off line to prevent unwanted disclosure of corporate data. Electronic Vaulting is currently more expensive than traditional data storage, primarily due to transmission charges.[47]

Vital Records Storage and Recovery

In addition to backing up electronic media and data, companies are also dependent on paper records for survival, records that are at risk during disasters. A Company or organization will often have legal or contractual requirements to maintain records and be able to retrieve them if needed. Many organizations archive their records in warehouses, basements, or other areas prone to disasters. As the records are not currently used for operations, and are not producing income they are relegated to any available space. Other corporations have hired a vendor to store and archive their records. Likely, the vendor's facility will not be much better than the originators and may lack adequate fire, flood, and wind protections.

Although great care should be taken in the storage of vital printed records, many organizations, especially government, will not heed the warnings of experts. Imagine how many records are stored in county courthouses, federal buildings and the like and are susceptible to water, fire and smoke damage. In the event of a disaster striking printed records there are options for recovering and restoring the records to a useable condition. Disaster Recovery Services Inc. of Ft Worth TX is an example of a company that specializes in printed document restorations and recovery. Disaster Recovery Services uses its large freeze dryers and other techniques to restore printed matter to a re-useable condition. Disaster Recovery Service is currently recovering over 500,000

volumes of historic bound material from a library flood in the western United States. Restoration of paper documents is a long and tedious process and may take several years to complete large projects.

Y2K-The Only Beneficial Aspect

The Millenium Bug has also impacted BCP. Planners are finding themselves tasked to develop plans and assist in conducting exercises to ensure Y2K compliance for the entity. This is a natural growth of the BCP realm and will likely provide an opportunity to demonstrate usefulness of the function to a broad range of personnel from the CEO to the Warehouse Manager. Y2K has brought a great deal of attention to BCP and sensitized people of security issues and especially service continuity.[48] The Millenium Bug cannot be taken lightly, it is a hard deadline which cannot be changed, and if systems are not compliant, or their back-ups fail, it will be the first ever disaster recovery that failed with years of advance knowledge to prevent such as disaster.

CASE STUDIES IN BUSINESS CONTINUITY PLANNING

Case Study: Large Metropolitan Area Transit Authority

Public Transportation is a critical commodity and function in a large metropolitan area. Every person in the society feels the impact of an efficient metropolitan transit authority, from a reduced load on the roadways to vehicle emissions saved when commuters use the rail system. A transit system is often the only mode of transportation available to residents of a metropolitan area and it's a lifeline the community depends on daily.

The Authority relies on two basic computerized systems. The operations system that controls rail movements and the administrative systems that process payroll, work orders, purchasing et cetera. The rail movements are controlled by a computerized system, which runs two mirrored systems. If one system goes down, the other system is able to immediately switch into control and function. If both systems go down, the rail operations are switched back to manual controls and the engineers take full control of the locomotives.

The administrative system controlling the business operations has a single time sensitive function that must operate in a disaster. Although the union that provides workers to the authority has a "no strike clause" in their contract, workers do have the choice of not reporting for work if they do not receive their

weekly paychecks. This fact made the payroll system a critical function that required a 24-hour recovery capability.

The workers are paid by the day and are paid every week. The payroll system has a detail to gross system which records every piece of work produced by one of the 6600 employees at approximately 80 work sites. This system amounts to over 80,000 recorded transactions per week that are compiled to produce paychecks for the employees.

The Business Continuity Planners went through every application and determined what was critical to support the payroll. They then developed a solution that includes the use of a vendor hot site in the local area. The hot site plan has been tested six times in exercises and has functioned well. In the event of a longer term disaster relating to computing functions, the authority also has the capability to move Accounts Payable functions as well as the General Ledger to the contracted hot site, however, a 72 hour lag time is necessary to move these functions.

Business Continuity Planning for the authority was primarily driven by a Department of Transportation Audit. The authority also uses an independent Certified Public Accounting firm who had also found the need for a BCP in audits. The Authority's plan is sound and will function well in the event of an outage or disaster.

Case Study: Financial Services Firm

The Firm is a congressionally chartered corporation that purchases loans from lenders and resells them to investors. The Firm's function in the economy is critical to ensuring the availability of funds for loans throughout the country. This 40 billion-dollar corporation has over 4,000 employees geographically distributed throughout the United States. The Firm is headquartered in the Washington DC area and has six loan servicing centers throughout the United States. Also distributed throughout the United States are six regional marketing offices and three specialized offices. The Firm currently has three Business Continuity Planners who have developed and implemented a mature recovery plan. The Business Continuity Plan is exercised on a semi-annual basis and has been successfully implemented to recover from both Natural and Technical Disasters. Each exercise encompasses over 150 persons and generally, the exercises are conducted for all data center platforms. Updates to the plan are a significant task and are accomplished annually.

The Firm uses a hot site vendor for data center support. The vendor provides a pre-determined location from which to support the firm in the event of a data center disaster. The Firm is limited in the available vendors for hot site selection as there are only a few sites that have the required computing capability. The Hot Site vendor has a $25,000 declaration fee for each disaster. The fee requires a corporate officer to declare the disaster, as the planning function does not have the requisite authority to bind the corporation

contractually. The Firm can make use of the Hot Site for six weeks, and then operations would move to a cold site that has been equipped in the interim between declaration and the end of six weeks.

The Firm manages their headquarters disaster response through the use of an Emergency Operations Center (EOC). When the EOC is activated, one of six vice-presidents with the requisite authority to declare a disaster reports and manages the EOC. The VPs determine the business impact of the current situation and recovery times are calculated. The impact of a disaster depends largely on the stage of the business cycle in which it occurs. If a disaster were to strike at the end of a quarter if could impact $5 billion dollars of transactions and cost over $500,000 in interest.

In addition to the lost interest, the firm also has critical customer service requirements. The Firm is obligated to send delinquency notices on schedule or risk losing the ability to collect on bad debts. In additions to these requirements there are due diligence and contractual requirements with banks that require business continuity plans.

In addition to the Headquarters plan, The Firm also has business continuity plans for each of their six loan servicing centers. The Loan Servicing Centers (LSC) are currently under reorganization and will be reduced to 4 centers with approximately 750 employees by September 1998. Each LSC also

has an Emergency Operations Center that is responsible for declaring and managing a disaster. Each function has a BCP that was developed by the people in the function with the assistance of the headquarters planners. The Headquarters is responsible for ensuring each LSC has an Emergency Response Plan and a Business Resumption Plan, and that the plans are tested and exercised. The Firm has gone to great lengths to ensure employees are prepared for the response required in an emergency. Every employee receives safety and emergency preparedness briefings on an annual basis.

When a disaster strikes a LSC, the headquarters dispatches a Crisis Management Team (CMT) to assist the local leadership in recovery efforts. The CMT brings assets from personnel, facilities, telecommunications and legal to the local area to ensure the local leadership has the resources required to resume operations.

The Firm is acutely aware of the impact of a natural disaster on employee's families and as a result has implemented significant assistance programs. During Hurricane Opal and the aftermath, The Firm automatically continued employee pay for 30 days. They also made available advances to support housing reconstruction or relocation. The Firm also brought in an insurance expert that helped employees interface with their personal insurance companies to ensure their employees received all of the benefits they were entitled to. After their Panama City, FL office was reopened, they allowed

employees to bring their families in to use the lavatory facilities and even allow children to stay with their parents during workdays. The Firm realizes that employees are their most important resource, and only by supporting their needs can they expect to resume operations in a timely manner.

The Headquarters disaster plan was also tested under actual conditions during a flood. When the Headquarters was located in a section of Washington DC, a flood caused the firm to relocate approximately 40 executives overnight. The executives were relocated and fully functional within 24 hours. Although the relocations were in the same geographical area, this event went a long way to prove the necessity and benefits of BCP.

The Firm's contingency planners have historically had robust budgets, which has led to excellent plans and seamless operations when disaster has struck. In recent years, The Firm has been forced to restructure workforce and reduce overhead and support budgets. As a result the contingency planning function has found its budget significantly reduced. Although the ever positive planners have made great strides in providing the same level of performance with less budget, the planners admit that it now takes longer to conduct exercises and they are often faced with innovating less expensive ways to achieve the same results. Overall the Firm has a solid plan and should continue to function well after a major disaster.

Conclusions

All organizations are dependent on People, Information, and Communications to conduct business. Interruptions that affect any of these resources will have a detrimental impact on business. Disasters that affect these resources will likely have a far-reaching impact on business and may result in the failure of the business or organization. Organizations must plan for continuing operations after a disaster via a Business Continuity Plan. The BCP is a critical function of the business and will impact every function of the business. Planners must have resources and commitment from senior executives to be successful. Planners must develop plans that recover time sensitive functions first, while bringing less time sensitive functions on line in an economically balanced manner. Planners must consider the toll of a disaster, not only on their facilities and equipment, but on the human resources which are their most precious asset. Planners must ensure plans are maintained and exercised on a regular basis and critique the exercise participants to improve their chances for successful resumption of business. Companies that put their people first and have experienced a disaster have more mature plans than their counterparts, however all companies need to plan for the inevitable.

ENDNOTES

[1] Ianna, Frank. Disaster Recovery for Business, Disaster Recovery Journal, Summer 1997, Volume 10 Issue 3, p 2.
[2] Wold, Geoffrey H. Disaster Recovery Planning Process. Part 1 of 3. Disaster Recovery Journal, Internet Resource. http://www.drj.com/new2dr/w2_002.htm
[3] Willumstand, Laura. Cigna Embarks on Corporate Wide Recovery Program to Protect Critical Locations Nationwide. Disaster Recovery Journal, Spring 1998, http://www.drj.com/articles/sp98/will.htm
[4] Willumstand, Laura. Cigna Embarks on Corporate Wide Recovery Program to Protect Critical Locations Nationwide. Disaster Recovery Journal, Spring 1998, http://www.drj.com/articles/sp98/will.htm
[5] Miora, Michael. The CIO's Role in Preparing for Disaster Recovery. Published in EDI World, 1995. Internet Resource. http://www.miora.com/art-cio.htm
[6] Miora, Michael. The CIO's Role in Preparing for Disaster Recovery. Published in EDI World, 1995. Internet Resource. http://www.miora.com/art-cio.htm
[7] Devlin, Edward S. Devlin and Associates. Personal Interview, Entire Section Excerpted from Interview
[8] Devlin, Edward S. Devlin and Associates. Personal Interview, Entire Section Excerpted from Interview
[9] Devlin, Edward S. Devlin and Associates. Personal Interview, Entire Section Excerpted from Interview
[10] Devlin, Edward S. Devlin and Associates. Personal Interview, Entire Section Excerpted from Interview
[11] Devlin, Edward S. Devlin and Associates. Personal Interview, Entire Section Excerpted from Interview
[12] Devlin, Edward S. Devlin and Associates. Personal Interview, Entire Section Excerpted from Interview
[13] Devlin, Edward S. Devlin and Associates. Personal Interview, Entire Section Excerpted from Interview
[14] Devlin, Edward S. Devlin and Associates. Personal Interview, Entire Section Excerpted from Interview
[15] Devlin, Edward S. Devlin and Associates. Personal Interview, Entire Section Excerpted from Interview
[16] Devlin, Edward S. Devlin and Associates. Personal Interview, Entire Section Excerpted from Interview
[17] Austin, Marshall H. (Marty). Peak Consulting Services, Woodbridge VA, Personal Interview
[18] Boltz, Jean. General Accounting Office, Project Manager, IRM Issues, Personal Interview
[19] Boltz, Jean. General Accounting Office, Project Manager, IRM Issues, Personal Interview
[20] Miora, Michael. The CIO's Role in Preparing for Disaster Recovery. Published in EDI World, 1995. Internet Resource. http://www.miora.com/art-cio.htm
[21] Boltz, Jean. General Accounting Office, Project Manager, IRM Issues, Personal Interview
[22] Learning from Leading Organizations, Information Security Management, Exposure Draft. November 1997, General Accounting Office.
[23] Patrowicz, Lucie Juneau, A River Runs Through IT, CIO-The Magazine for Information Executives, April 1, 1998, p40.
[24] Ianna, Frank. Disaster Recovery for Business, Disaster Recovery Journal, Summer 1997, Volume 10 Issue 3, p 1.
[25] Moore, Pat, Strohl Systems, Vice President of Business Continuity Education, Responses to Direct Questions via Electronic Mail
[26] Boltz, Jean. General Accounting Office, Project Manager, IRM Issues, Personal Interview
[27] Devlin, Edward S. Devlin and Associates. Personal Interview
[28] Moore, Pat, Strohl Systems, Vice President of Business Continuity Education, Responses to Direct Questions via Electronic Mail

[29] Moore, Pat, Strohl Systems, Vice President of Business Continuity Education, Responses to Direct Questions via Electronic Mail
[30] Devlin, Edward S. Devlin and Associates. Personal Interview
[31] Devlin, Edward S. Devlin and Associates. Personal Interview
[32] Patrowicz, Lucie Juneau, A River Runs Through IT, CIO-The Magazine for Information Executives, April 1, 1998, p40.
[33] Devlin, Edward S. Devlin and Associates. Personal Interview
[34] Devlin, Edward S. Devlin and Associates. Personal Interview
[35] Glancy, Christopher and Stamieszkin Piotrek, How to Develop A Comprehensive Business Resumption Plan at a Large Organization, Disaster Recovery Journal, Volume 10 Issue 3, Summer 1997, p 2.
[36] Devlin, Edward S. Devlin and Associates. Personal Interview
[37] Wold, Geoffrey H and Shriver, Robert F. Risk Analysis Techniques, Disaster Recovery Journal, Internet Resource. http://www.drj.com/new2dr/w3_030.htm
[38] Wold, Geoffrey H. Disaster Recovery Planning Process. Part 1 of 3. Disaster Recovery Journal, Internet Resource. http://www.drj.com/new2dr/w2_002.htm
[39] Wold, Geoffrey H. Disaster Recovery Planning Process. Part 3 of 3. Disaster Recovery Journal, Internet Resource. http://www.drj.com/new2dr/w2_004.htm
[40] Wold, Geoffrey H. Disaster Recovery Planning Process. Part 3 of 3. Disaster Recovery Journal, Internet Resource. http://www.drj.com/new2dr/w2_004.htm
[41] Wold, Geoffrey H. Disaster Recovery Planning Process. Part 3 of 3. Disaster Recovery Journal, Internet Resource. http://www.drj.com/new2dr/w2_004.htm
[42] Devlin, Edward S. Devlin and Associates. Personal Interview
[43] Schaming, Joan T. What Is This Thing Called Risk Management, Disaster Resource Guide, 1998 Edition, p 27.
[44] Austin, Marshall H. (Marty). Peak Consulting Services, Woodbridge VA, Personal Interview
[45] Austin, Marshall H. (Marty). Peak Consulting Services, Woodbridge VA, Personal Interview
[46] Austin, Marshall H. (Marty). Peak Consulting Services, Woodbridge VA, Personal Interview
[47] Koski, Kevin. WhatYou Need to Know About Electronic Vaulting, Disaster Recovery Journal, Winter 1998
[48] Boltz, Jean. General Accounting Office, Project Manager, IRM Issues, Personal Interview

Blank Paper for Comments